Title: PNR agreement with Canada not cleared for takeoff

Author: Fanny Coudert

11 October 2016, https://www.law.kuleuven.be/citip/blog/pnr-agreement-with-canada-not-cleared-for-takeoff/

Key words: police, law enforcement, privacy, data protection, PNR, profiling, mass surveillance, Digital Rights Ireland

Categories: Data protection / Security&Crime

Abstract: *On the 8th of September, AG Mengozzi issued his Opinion in the first case brought to the CJEU on the validity of an international agreement in light of the EU Charter. The European Parliament referred the text of the PNR Agreement with Canada before approving the proposal of the Council. This case also gives the Court the opportunity to further specify the criteria that should regulate the mass collection by law enforcement authorities of data captured by the private sector in their day-to-day business. The case is situated in the line of other cases brought before the CJEU (Digital Rights Ireland, Schrems) and the ECtHR (Zakharov and Szabó).*

The agreement under scrutiny provides that Passenger Name Record data (PNR data), collected by airlines during the reservation of flights between the European Union and Canada, are to be transferred to Canadian law enforcement authorities (LEAs) for the prevention of terrorism and other serious crimes. The data are then run against intelligence to identify patterns of behaviour that will allow to spot high-risk individuals, in particular individuals unknown to police forces.

Similar agreements have already been passed with the United States and Australia. A European PNR system was also made possible by the recently adopted Directive (EU) 2016/681. However, bulk data transfers to LEAs are, since the Digital Rights Ireland judgement, under the strict scrutiny of the Courts. These transfers are indeed "capable of giving the unfortunate impression that all the passengers concerned [or users of electronic communication services in the Digital Rights Ireland case] are transformed into potential suspects" (Opinion, §176).

These cases are symptomatic of a new logic emerging in the field of law enforcement, according to which "in order for the suspect to emerge, everyone must be subject to surveillance". The ECtHR also recently dealt with a series of surveillance laws that gave law enforcement broad surveillance powers in Zakharov and Szabó. Big data technologies give LEAs the capability to process vast amounts of data, to monitor whole populations and focus on individuals that algorithms have identified as "of concern" or as "presenting an "interest"(Opinion, §164) .

Both the CJEU and the ECtHR acknowledge that the use of extremely sophisticated methods to monitor the private life of individuals and analyse their personal data is inevitable (Opinion, §8, Szabó, §68). However, the massive scale at which surveillance takes place forces them to revisit the safeguards initially put in place to protect against an "unfettered use of powers" (Szabó, §70). As cases flow to the courts, they progressively shape the contours of what "proportionate" and

"foreseeable" interferences mean. They draw the limits between acceptable and unacceptable mass surveillance practices.

A strict necessity test

The AG performs a detailed proportionality test, further specifying the requirement of "strict necessity" of the interference, based on the criteria set up by the ECtHR. In light of his assessment, a number of provisions relating to the scope of the agreement (offences and information falling under the different categories of data) and the criteria used for the profiling (databases used to cross-check the data and scenarios and risk assessment criteria) should be defined more precisely. The agreement should include a detailed list of data, offences, or recipients. The AG also applies a strict necessity test to each of the categories of data to be transferred or retained. He considers that sensitive data should be excluded from the scope of the transfer as their added-value has not been demostrated. He also considers that data retention periods must be based on objective criteria and be differentiated. It is not sufficient to only mention that the data retention period is linked to the average lifetime of international serious crime networks and the duration and complexity of investigations of those networks. Furthermore, certain categories of data might not need such a long data retention period such as for instance, the frequent flyer and benefit information or information about the check-in status.

Strong oversight mechanisms

The AG also reviews the oversight mechanisms put in place. The authority responsible for processing PNR data should be clearly defined in the agreement and provide sufficient guarantees of independence. An authority which is directly subordinated to a Minister from whom it may receive direction does not meet this criteria.

As regard the nature of the oversight, the AG recalls that *ex ante* control (in the sense of prior authorisation) is not absolutetly necessary, provided extensive *ex post* judicial oversight is guaranteed, i.e. there is a review of the decisions or actions relating to access to PNR data. Yet, he recommends that the supervisory authority periodically checks the relevance and proportionality of the databases used to cross-check the data and of the risk assessment criteria. The supervisory authority must verify that these make it possible to arrive at results targeting individuals who might be under a "reasonable suspicion" of participating in terrorism or serious transnational crime. This autority should further share its report with the competent institutions and bodies of the Union.

The AG also recommends that European Commission and the concerned Member State should be notified of any disclosure of PNR data to other Canadian governmental authorities or to third countries. Onward transfers will indeed refer to individuals who are under sufficient (criminal) suspicion, on the basis of the analysis. The impact is such as a mere *ex post* control does not appear sufficient. The AG strongly advises that Canadian authorities are not the only ones assessing the necessity and adequate level of protection afforded by the recipients in each individual case.

A new set of criteria?

In conclusion, this Opinion provides useful guidance as to the content of safeguards limiting the margin of discretion of public authorities with regard to bulk data transfers from the private sector to LEAs. At a time when the EU is implementing its own PNR system, the ruling will shed a welcome

light on specific safeguards that should be put in place, complementing the EU PNR Directive. It will also provide useful insights for Member States which decided to maintain their national system of retention of electronic communications for law enforcement purposes.